GSMK CryptoPhone 300
with SMS Encryption

User Manual

Version 1.00, build 129

GSMK CryptoPhone
8:06
New Message
Inbox
Lock
Settings
Contacts
Secure Call
Folders

Main Screen

General 5
Inserting SIM card & switching the phone on 5
Security Profile Manager 6
Enter your PIN 11
Secure Storage 11
Changing the Passphrase 13
The Secure Contacts list 13
Locking the Secure Storage 14
Charging 15
Standby 16
Switching on/off 16
Key Verification 19
Redialing 19
Call Quality during Secure Calls 20
Secure Calls while moving 21
Switching the Calltype 22
Switching the Linetype 23
Problems with setting up a Secure Call 24
Changing the volume 26

Mute during call 26
General Mobile Phone Security Advice 26
CryptoPhone SMS 27
Key Exchange for CryptoPhone SMS 27
Sending CryptoPhone SMS 30
Receiving CryptoPhone SMS 31
Emergency Erase 32
Security Advice regarding Flash Storage 34
Using the headset 35
Bluetooth headset 35
Sync Contacts and Appointments 36
Troubleshooting 37
Security Updates 37
Security Advice 39
Storage and Handling 40
Repairs 40
Accessories 41
3rd Party Software 41
Known Issues 42

9. During key exchange, the calculation and verification of the Diffie-Hellman parameters takes a while, with the “spinning ball” wait cursor shown. Just wait till it disappears.

10. Locking of Secure Storage on standby does not work reliably. The storage locks automatically after the set number of minutes since the last unlock has passed, not since the last activity on device (as it should).

11. Graphics artifacts may remain for a few seconds when switching between landscape and portrait mode while the device is busy.

12. Emergency Erase does **not** delete everything outside the Secure Storage. Normal SMS and Contacts in Outlook may remain. There are “Out of System Memory” messages during Emergency Erase. The counter-forensics hardness of the Emergency Erase has not been severely tested for other things then the Secure Storage.

13. If you press Invite instead of Save for a new contact that you just have entered, the invitation to key exchange is sent out, but the contact is not saved. Please always save a new contact before inviting it to key exchange.

General

Your CryptoPhone 300 is based on a quadband (850/900/1800/1900) GSM PDA-phone hardware that is sold under different brand names. The phones firmware and operating system have been modified to accommodate the CryptoPhone functionality and provide added security, so a number of things that you might know from other Smartphones are different on the GSMK CryptoPhone for security reasons. The original Smartphone manuals, license sticker and CD are supplied with the GSMK CryptoPhone 300, but you need to be aware that some functionality has been disabled for security reasons and some functions have been changed to better integrate the CryptoPhone functionality. Do not try to use Microsoft or HTC system updates as this will destroy the CryptoPhone firmware and void your warranty. Certified CryptoPhone Updates are only provided by GSMK to you in a cryptographically secure manner.

Inserting SIM card & switching the phone on

On the lower small side of the phone is a small lock/unlock latch. Move it to the open lock symbol. Now you can flip open the back cover of the phone. Remove the battery by flipping it on the small handle to the right side. Then click down the SIM holder as indicated by the arrow and insert the SIM. Close the SIM holder and insert the battery. Now reattach the back cover and switch the back cover latch to the locked position. Switch on the phone pressing the power button on the upper small side of the phone.

Security Profile Manager

The CryptoPhone is based on the Windows Mobile operating system which contains some potentially vulnerable, yet convenient features and applications. To reduce the risk of attacks against your CryptoPhones integrity, it is recommend to disable some of these features. The Security Profile Manager helps you to select between security and extra features: the more features you enable, the larger the risk of vulnerabilities. In the following the different settings of the Security Profile Manager are explained in detail. Please take your time to read all the options to make a informed decision. After you have selected a Security Profile, click the OK button on the screen. Now the phone will install the operating system components according to the profile you selected.

The default setting is "Medium Security" which provides a good balance of convenience and security for most users.

Note: You can always change the Security Profile setting by performing a Hard Reset (see separate phone hardware manual). After each Hard Reset you will be asked for your choice of Security Settings.

The available Security Profile choices are explained below in detail.

comfortable encrypted group messaging feature will be provided in one of the next releases.

2. There is no counter that shows the number of characters left in the message. You can type long messages anyway, they will be sent as multiple SMS automatically.

3. Reassembly of long messages does not work properly. Long messages are shown as two or more messages at the recipients side.

4. Message compression is currently not optimal.

5. The contacts import function has some problems importing numbers other then the mobile number. Please make sure that you store the number of the partner that you want to send SMS to or call secure as the Mobile number before importing.

6. There is currently no method to send contact details by encrypted SMS.

7. In the Security Manager setting Extreme Security, also CryptoPhone SMS will not work.

8. Mute and V.32 indicators are not shown in landscape view of the CryptoPhone.

that installing 3rd party software might irrevocably compromise the security of your CryptoPhone or damage its functionality.

GSMK does not provide any support for installing 3rd party software and will not provide support for problems caused by installing 3rd party software. Any and all problems caused by 3rd party software are not covered by warranty or support.

You have been warned.

If you require large number of custom CryptoPhones that include certain software components of your choice by default, please contact sales@cryptophone.de to discuss your requirements.

Known Issues

The following issues and problems are known for the GSMK CryptoPhone 300, Version 1.00 built 129. Some issues may have been solved already in the firmware version on your phone. You can check your firmware version under Settings --> About.

1. Encrypted SMS can only have one recipient at this time. If you need to send the same SMS to multiple persons, save the message to Drafts (Menu --> Save to Drafts) before sending and send it multiple times from the Drafts Folder. An

No Added Security

This setting leaves the CryptoPhone with very little protection against potential attacks on the operating system. Some mechanisms to prevent really stupid attacks are activated, but this creates only a base layer of protection that is not sufficient against a skilled adversary. New threats (against any operating system) are discovered from time to time, selecting "No Added Security" exposes the CryptoPhone to non necessary risk. Choose this setting only if you really need one of the services that would otherwise be disabled in the "Medium security" setting and if doing so matches your risk profile. The following functionality has been disabled even in No Added Security mode, because the risk is too high:

- MMS receiving
- SIM-Toolkit

Medium Security

At this level of security, the CryptoPhone disables a number of functions which are likely vulnerable to attacks, but are not essential for most users. Once you select Medium Security, the following functionality is disabled:

- Picture Caller ID and Picture Contacts
- .NET compact framework
- Javascript
- MIDP and all other Java framework
- MS scripting
- VBscript
- MS terminal services client
- MS Messenger client
- SIM Toolkit
- Remote OS updates
- Downloadable Ringtones
- some media playback features
- WAP and WAP push
- MMS and Video-MMS

proper shipping and security procedures. Shipments that arrive for repair without prior acknowledgment and/or in ignorance of the advised shipping method and security precautions will be ignored. Please understand that it is in your own interest to adhere to the security measures, since only this will enable GSMK to fulfill your security requirements. Note: the high-power Lithium-Polymer rechargeable battery of the CryptoPhone is a wear-and-tear part and not covered by the warranty. Replacement batteries are available in normal PDA or mobile phone stores.

Accessories

The GSMK CryptoPhone is based on a device manufactured by HTC, sold under different brand names. Additional accessories for your CryptoPhone (like holsters, car kits etc.) can therefore be easily obtained by buying equipment that is destined for HTC P4350 devices.

3rd Party Software

In theory it is possible to install Microsoft Smartphone compatible 3rd party software on your GSMK CryptoPhone device. You should know that 3rd party software of any kind can be used to attack the integrity and security of your GSMK CryptoPhone. Installing additional software on Communication Security equipment like the CryptoPhone is a grave security risk that you should only take if it is absolutely necessary. Please be aware

Storage and Handling

The CryptoPhone is specified and designed for use in normal business, home and other general conditions. It is not reinforced or specially sealed against water and other harsh environmental conditions. (For reinforced versions of the CryptoPhone that comply with military specifications, contact sales@cryptophone.de). Submitting the CryptoPhone to excessively high or low temperatures (like in the outside pocket of an overcoat in cold climates) might temporarily or permanently damage the display and lead to accelerated battery aging, affecting the ability of the battery to store power and thereby reducing the standby time of your CryptoPhone. Sitting on the CryptoPhone or submitting the device to other heavy mechanical loads may damage parts of the phone, especially the keyboard. Damage to the keyboard, battery and display as well as any kind of other mechanical damage is not covered by the warranty.

Repairs

Because of the manipulation risk, GSMK does not take back any CryptoPhones from customers, except for repairs. There is no such thing as a »restocked«, »refurbished« or »second hand« CryptoPhone. All sales are final. If your CryptoPhone is defective, GSMK will either repair it or swap the electronics for a new factory fresh device. No parts that have been in the hands of other customers will be used in repairs. If you need a repair, please mail to service@cryptophone.de. You will then receive instructions about the

High Security

In the High Security mode, internet functionality is no longer avaialble. GPRS, PPP data calls, the Internet Explorer and the Windows Media Player are disabled, in addition to the measures taken with Medium Securty. The following functionallity is disabled in High Security mode:

- Bluetooth
- OBEX
- WLAN
- GPRS
- all TCP/IP funcitonality
- Mediaplayer
- Internet Explorer
- Video Telephony
- some email functionality
- ActiveSync
- Infrared
- some SD-card functionality

Extreme Security

This setting is intended for customers who only use the CryptoPhone and normal unsecure call functionality, but wish to have all other means of communication disabled. This security level offers protection against attacks that potentially could be performed using SMS messages or the synchronization with a desktop PC. PocketOutlook, SMS sending and receiving, Active Sync and the Inbox are disabled in this setting, in addition to the measures taken in High Security mode. This setting is recommend for situations where a highly skilled adversary has to be assumed.

Note: Depending on how you obtained your CryptoPhone, not all Security Profiles might be available or the described choices might be different in detail. GSMK provides customized Security Profile configurations as part of volume purchases for larger companies and organizations. So if you received your CryptoPhone from your organization, please consult with the appropriate corporate security manager regarding the choice of Security Profiles available to you. Also, GSMK may, without notice, remove certain components from the default installation, if information becomes available that indicate a higher then originally assumed vulnerability of this component.

immediately, as this may be an attempt to insert malicious firmware into your CryptoPhone. Please see the Questions and Answers section (Q&A) on the website http://www.cryptophone.com/ for further detailed information on the benefits of published source cryptography.

Security Advice

Your CryptoPhone is a Communication Security (COMSEC) device. It can only be regarded as secure as long as you have permanent and uninterrupted physical control over the CryptoPhone. Once an adversary could have gained temporary physical possession of the CryptoPhone, it must be regarded as compromised. There is a variety of potential methods that would allow an adversary to listen into your calls after he manipulated the CryptoPhone and gave it back to you. Keep the handset with you securely at all times. Optimally, you should take it with you to the bathroom, put it beside your bed when you sleep and not leave it alone in the hotel room.

If you have »lost« the CryptoPhone and »find« it back again, it has to be regarded as compromised. Never lend your CryptoPhone. Major intelligence agencies are known for a wide variety of high-tech manipulation methods that are impossible to detect without a massive scientific effort (several months of analysis at the cost of several 100.000 Euros per device). If in doubt and your security depends on it, consider purchasing a fresh unit.

Security is not a state but a process. And this process requires constant checking against emerging risks and new attack methods. Since the CryptoPhone comes with full published source code, the chances are much higher for a flaw to be discovered and fixed quickly than with any closed-source cryptographic product. An advisory board of distinguished cryptographers and security researchers helps to identify and counter potential threats based on their intimate knowledge of the latest academic research and emerging cryptanalysis methods. In case a firmware update is needed for security reasons, you will get notified either via the e-mail address that you supplied when purchasing the CryptoPhone online, or directly by your local authorized CryptoPhone distributor.

If you receive a notice about an upcoming security update, please verify it by contacting GSMK directly. The contact details are listed on the website http://www.cryptophone.com/ to prevent attackers from slipping you a malicious »update«.

The firmware update mechanism is cryptographically secured using a 4096 bit public key signature system, which ensures only signed CryptoPhone updates will be accepted by your CryptoPhone.

If you receive suspicious communication regarding CryptoPhone updates (such as an unannounced e-mail with an update file as attachment), please inform GSMK

Enter your PIN

Most GSM SIM cards require you to enter a PIN number. After you have switched on the CryptoPhone, you will be asked to enter your PIN. After you entered the PIN, press the “Done” button. The CryptoPhone will finish initialization and provide the secure telephony mode. If your GSM SIM does not require a PIN, the secure telephony mode will be enabled right away.

Note: It is recommend that a PIN number is used, as it makes the extraction of information stored on the SIM more difficult for an attacker and prevents you from incurring charges to your account if the phone is stolen.

Secure Storage

The CryptoPhone 300 provides an encrypted storage system to store all contacts, and associated information like the keys for SMS encryption secured against unauthorized access. The information in the Secure Storage is encrypted with the same strength of cryptography and the same key length as CryptoPhone Calls and CryptoPhone SMS. However, the ultimate strength of the protection is dependent on the quality and length of your passphrase.

Upon first use, you will be asked to enter a passphrase for the Secure Storage. This passphrase is used to cryptographically protect a key, that is then used to encrypt and decrypt the data in the Secure Storage. **If an adversary gets access to your CryptoPhone 300, the security of your Secure Storage which stores contacts, encrypted SMS and associated information depends entirely on the strength of your passphrase.**

It is strongly recommended to choose a passphrase of at least 16 characters that is very difficult to guess, using upper- and lowercase letters, non-standard characters and numbers. An easy way to remember a strong passphrase is to use a poem or verse, leaving out spaces and substituting some letters with numbers. Another good memory trick is to take a memorable sentence and use only the first or last letters of the words as passphrase. If you choose a passphrase that is just one or a combination of simple words, an adversary can simply use a computer that automatically tries out words and word combinations from a huge dictionary and will find your passphrase, thus compromising your stored information.

future. The main risk is that an adversary could potentially gain wireless access to your device while it is in your pocket or just on the desk in front of you.

Troubleshooting

In the event that the CryptoPhone reacts unexpectedly i.e., device response becomes very slow or the phone does not connect to a GSM network, you can quickly reset it by pushing the reset button on the left side of the device with the stylus. The GSMK CryptoPhone will restart without erasing the memory. In the unlikely event such a problem persists, you can Hard Reset the device. This will however delete (not overwrite) all information in memory, including all information in the Secure Storage.

Security Updates

GSMK continually seeks to improve the security and quality of operation of the CryptoPhone 300. In the event anyone discovers a flaw in the CryptoPhone, GSMK will provide a firmware update, as well as a detailed report on the possible security impact. As bad as security problems with cryptographic products can be, GSMK believes the only way to handle them properly is open and transparent communication with customers. You are the one best suited to determine potential damage to your interests, so you will be provided with all the known facts to make an informed decision.

offer sufficient protection. A wire based headset is your best option when placing secure calls.

Sync Contacts and Appointments

The CryptoPhone supports in principle the sync of contact and calendar entries with a computer. You need to be aware that in theory it might be possible to attack the operating system of the CryptoPhone by supplying manipulated data to your PC or exploiting unknown problems in
ActiveSync. GSMK does not recommend to sync your CryptoPhone with a PC, especially if the PC is connected to a network, for security reasons. If you have high security demands and need to calculate with a very sophisticated adversary, avoid to sync your CryptoPhone with a PC. The CryptoPhone ships with de-activated Active Sync functionality. You need to re-activate the sync option manually in the CryptoPhone to use it. To initiate a sync, connect the CryptoPhone with the computer using the enclosed USB cable. When you sync your CryptoPhone with a PC, your should physically disconnect the PC from any network connection as a precautionary measure.

Note: Sync over IrDa (Infrared) and Bluetooth has been deactivated on the CryptoPhone as a precautionary security measure. You may re-activate it if desired when you need to sync you r phone with a PC. While GSMK is currently not aware of actual problems with these sync options, there is a very strong likelihood that such problems will arise in the

Changing the Passphrase

To change the passphrase for the secure storage, use the Settings icon in the Main Screen and select the Change Passphrase button in the Storage tab. You will need to enter your old passphrase first. **Note: A lost passphrase can not be recovered.**

The Secure Contacts list

In addition to the standard contacts list in the operating system, the CryptoPhone 300 is offering an encrypted CryptoPhone Contacts list that stores your contacts in the Secure Storage. It is recommended to use the Secure Contacts to prevent an adversary who may get your phone into his hands from gaining knowledge whom you are communicating with.

To import the contacts from your SIM and the standard phone contacts, go to Contacts from the Main Screen and select “Import Contacts” from the Menu. You can also delete contacts from the Menu and change the sorting to display your contacts according to keying status. To call a contact stored in the contact list, select “Contacts” in the CryptoPhone main screen, choose a contact. Now you see the list of contacts stored in the Secure Storage. Select the desired contact, press Menu and chose Call Secure. The encrypted call to the selected contact is then set up immediately.

To add a contact, choose New Contact from the Menu in the Secure Contacts screen. Enter the contact details and press Save before trying to invite the new contact to a key exchange.

Locking the Secure Storage

The Secure Storage provides protection for your SMS keys, encrypted messages and Secure Contacts only when it is locked. The Secure Storage can be locked in two ways. Either you lock it manually by using the Lock icon in the Main Screen after you are done using the data in it. Alternatively there is an automatic locking mechanism the Storage tab under the Settings icon in the Main Screen. You can choose to lock the Secure Storage after a certain number of minutes has been passed since the last unlock.

You should make sure that the Secure Storage is only unlocked in situations where you can be reasonably certain about the risk of your device getting lost. In an emergency, use the Lock icon in the Main Screen to quickly lock the Secure Storage.

Consider an Emergency Erase if you fear immediate capture of the phone by an adversary with advanced technical capabilities or if your passphrase is weaker then 16 alphanumeric characters.

The Secure Storage of the CryptoPhone 300 is built with these problems in mind and stores information only in encrypted form, so all the CryptoPhone contacts and CryptoPhone SMS are as secure as your passphrase is.

Using the headset

For hands free operation, a stereo headset is included with the GSMK CryptoPhone. You can plug it in any time, before or during a call, however you may terminate an ongoing call under some conditions when inserting the headset plug off-angle. The headset cable connector socket is on the right side of the device. GSMK does not provide support for problems caused by using headsets other than the one supplied with your CryptoPhone.

Bluetooth headset

The CryptoPhone 300 has a Bluetooth interface. While it is possible to use a Bluetooth headset for making normal unencrypted phone calls in the lower Security Manager settings, it is strongly not recommend using a bluetooth headset during encrypted calls. The reason is that with a Bluetooth headset you would broadcast the contents of your confidential calls before they have reached the encryption engine in the CryptoPhone. Bluetooth radio signals can be received over several hundred meters and decrypted with moderately sophisticated equipment, so an attacker could listen to your calls easily. The encryption used with Bluetooth is no hurdle for a determined adversary and does not

for the call is destroyed and permanently erased. For CryptoPhone SMS, key material is stored in the Secure Storage with a method that is called “forward hashing”, meaning that only keys not yet used are kept. Keys for CryptoPhone SMS that have already be sent or received and decrypted

Security Advice regarding Flash Storage

With the GSMK CryptoPhone a lot of information is stored in Flash Storage. Flash type storage is safe against failure of the backup-battery. You must however be aware that except for the Emergency Erase there is no way to securely erase information stored in flash memory in a way that it cannot be possibly reconstructed by sophisticated methods of computer forensics. Flash memory uses its own way of managing data that is beyond the control of the operating system. This can lead to information residue being left, even after you deleted the file or information entry in the operating system.

So files that are no longer visible after deletion in the file manager may still exist in some unused part of the Flash memory. In addition, esoteric physical effects ("memory burn in") may make it possible for a forensic intelligence laboratory to reconstruct the former content of Flash memory, even if it has been erased or overwritten once. The same problem holds true for (mini)SD memory cards, because they are also based on flash memory technology.

Charging

Before using your CryptoPhone, it is recommend that you charge the battery until full. In order to do this, you must connect the power supply to the CryptoPhone. Depending on your location, you may need a plug adaptor to use the power supply if the plug does not fit in your outlet. The power supply is rated 100-240V, which means it will accept your line voltage without conversion as long as it lies within this range. The status LED will change color to orange while the device is being charged, and to green when fully charged. You can either charge the CryptoPhone with the power supply (recommended) or with the supplied USB sync cable on a computer. Charging over USB takes considerably more time and is dependent on your computers configuration and setup, so it may not work under some circumstances (e.g. if you have no synchronization software installed on your computer or the USB port is not powered up).

Due to the higher power consumption of the built-in powerful processor and the backlit display, the standby and talk times in secure mode are slightly less than what you might expect from normal GSM phones. Also please note that the standby and talk times may vary depending on your distance to the nearest GSM base station: the further away the base station, the more power your phone needs to use to reach it. Spare batteries are available in normal electronic stores that sell mobile phones.

Note: For security reasons explained later in the chapter 'Security, Storage and Handling,' it is recommended that you keep the CryptoPhone with you at all times so that it is under your permanent supervision. If the phone rings or you need to place a call while the phone is charging, you can leave it plugged in while operating the phone.

Standby

The GSMK CryptoPhone has three basic modes of operation. It can be either completely switched off, in 'standby mode' or active. In normal operation the CryptoPhone is in 'standby mode.' In standby mode, you can activate the device at any time by pressing the power button briefly.

Now the screen will light up. To put the GSMK CryptoPhone 300 back in standby mode, press the power button again. The GSMK CryptoPhone will still receive incoming calls when it is in Standby mode. In other words: standby mode will not disable the radio, it just puts the processor to sleep and switches the display off.

Switching on/off

It is not safe to enter an airplane, hospital or other no-phone area with the GSMK CryptoPhone switched on or in standby mode. To ensure the radio is off, you need to switch off your CryptoPhone 300 by pressing the power button for a few seconds. A

messages not yet received. In some situations you may be forced to hand over your passphrase by legal or illegal means. To provide you with an option to protect your data and keys in this kind of situation, the Emergency Erase has been designed.

Emergency Erase will erase all data stored in the Secure Storage that might compromise your security). The Emergency Erase is final and non-recoverable. The function continuously overwrites the writable internal Flash memory of the CryptoPhone 300 with random data.

Note that Emergency Erase will need to run for at least 3 minutes to make sure that the memory of the device has been completely overwritten. This is due to the slow write speed of the Flash memory. The complete overwrite of all flash memory is necessary, because traces of your data might otherwise be reconstructed by a skilled adversary by means of advanced computer forensics.

Emergency Erase will **not** securely overwrite the contacts and SMS messages stored in the normal Outlook/ Inbox and will also **not** overwrite SD-Cards present in the phone. However, these messages are at least deleted by the cold boot that happens after the Emergency Erase.

Note: No key material that might compromise the security of your past CryptoPhone calls is stored anywhere on your device. Upon completion of a secure call, all key material

When you have unlocked the Secure Storage, the SMS is automatically decrypted and stored in the CryptoPhone Inbox, which resides in the encrypted Secure Storage. This means that the SMS you received and decrypted can not be accessed by an attacker, even if you loose your device, as long as the attacker can not guess your passphrase.

A method to restrict the storage of messages is the “Eyes Only”-option, which can be set by the sender of the CryptoPhone SMS. SMS with the “Eyes Only”-flag can only be viewed immediately after decryption and will self-destruct after you read it. You can distinguish a “Eyes Only”-SMS by its little flame symbol on the letter icon.

Emergency Erase

To trigger an emergecny erase, go from the main screen to Lock and click the button labeled Emergency Erase. If the Secure Storage is locked, unlock it first.

The Emergency Erase function has been designed for true emergency situations, when the capture of your phone by an adversary is imminent and you would rather loose all your data then run any risk of your passphrase being compromised. While the Secure Storage provides protection against data compromise, this protection is only as strong as your passphrase is. If the adversary can guess your passphrase or find it by systematic computerized try out (brute force), he will be able to break into the secure storage and get access to your stored messages, contacts information and the SMS encryption keys for

request will pop up, asking you if you really want to switch off. To switch it on again, press power for two seconds. You will be required to enter your PIN again.
For flight mode and other options to switch wireless components on and off, please refer to the separate hardware manual.

After you switch your CryptoPhone on, it will start directly into the secure phone call mode.

To get to the Main Screen, minimize the secure phone screen by clicking the X icon in the upper right corner. Placing an Encrypted Call

In order to place a secure call, the following conditions need to be met:

- your partner has a CryptoPhone compatible device up and running
- there is sufficient GSM coverage
- the GSM operator supports ‘GSM data calls’ (technically called 9600 bit/s Circuit Switched Data or ‘CSD’)

To place a secure call, choose “Contacts” in the CryptoPhone main screen, select a contact and press the green button. You can also dial directly by selecting the “Call” icon,

enter the desired number and press the green button. You can always switch to the CryptoPhone main screen by pressing the center button for a second.

The very first call after you switch on the CryptoPhone will take longer to be dialed after you press the green button, as the random number generator needs to be initialized and

verified. After this you will hear a bit of comfort noise in the speaker, followed by the normal ringing tone. It may take longer than normal before the secure connection is made, so please let it ring. After your partner has pressed the Talk button on his end, you will hear a ditt-dutt ditt-dutt sound that signals to you that the 'key setup' procedure for the secure connection is in progress. Key setup may take from 3 to 30 seconds, but typically 4 seconds, depending on line quality. Once key setup is completed you hear a »Ping« sound and can start talking to your partner. In order to verify the authenticity of the key, Please take a look at the display and read the three letters under »you say« to your partner and verify the three letters under »partner says«. The green SECURE indicator is only visible when a secure call is established.

During all other times it is shown in grey with a open lock.

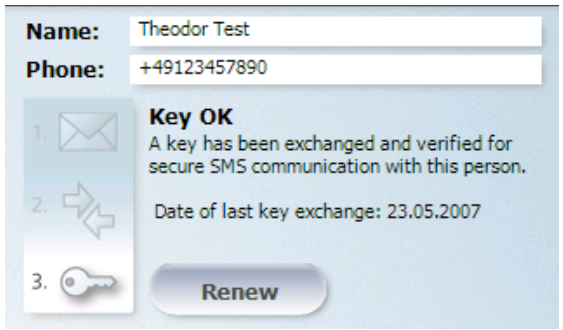
There are two ways to compose and address a CryptoPhone SMS. You can select the "New Message" Icon from the main screen, and select the desired recipient in the message compose screen via Menu --> Add Recipient.

The second method is to select the recipient from the CryptoPhone Contacts list and press the "Send Message" softkey. To add a recipient, use Menu --> Add Recipient in the message compose screen.

You can now compose and edit your message. CryptoPhone SMS supports long messages that are sent as multiple chained SMS. You can also use local language characters, as the messages are encoded in Unicode format.

Receiving CryptoPhone SMS

CryptoPhone SMS can be received whenever the phone is reachable in the network. You need to have a valid set of keys with your communication partner, meaning that you need to have completed the key exchange procedure with your partner. The decryption of CryptoPhone SMS is only possible when the Secure Stotrage is not locked, as the keys for the decryption are stored there. If an encrypted SMS is coming in and the Secure Storage is locked, you will be asked to unlock it. You can do that at a time convenient for you, the CryptoPhone SMS will be stored until then as it has been sent by your partner in encrypted form.



Note: CryptoPhone SMS encryption uses very long keys (4096 bit Diffie-Hellman, 256 bit AES & Twofish), to provide your communications with the best protection available. These long keys require substantial amounts of bits to be exchanged between you and your partner during the key exchange. One key exchange consists of six SMS sent by the inviting party and five SMS send by the invited party. The key exchange needs to be conducted only the first time when you start communicating with a partner. It can be renewed when required.

Sending CryptoPhone SMS

To send an encrypted SMS, you need to have a valid key for the recipient, meaning that you need to have performed the key exchange process outlined above successfully.

Key Verification

Reading the three letters and verifying what your partner says is meant to protect you against so-called 'man-in-the-middle attacks' on the secret session key. The session key is different for each call, as no key material is re-used between calls. The letters are mathematically derived from the unique secret key that is generated for each call. By reading and verifying them with your partner, you make sure that you are indeed communicating using the same key. Please pay attention to the voice of your partner when he reads his three letters. To be completely on the safe side against very sophisticated voice impersonation during the key verification, you could periodically reverify the letter code with your partner during the conversation.

Redialing

The CryptoPhone has access to a call history comprising the last 10 outgoing calls.. You can redial a number by scrolling through the last dialed numbers pressing the up and down buttons in the CryptoPhone screen and press the green Talk button once the desired number is shown in the display.

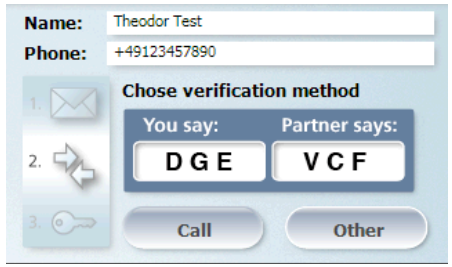
Call Quality during Secure Calls

The call delay indicator changes color in five steps between green over yellow to red. Green indicates the best call quality, red the worst.

Delay describes the period of time it takes for your voice to reach your partner. This time gets longer if the transmission of the encrypted voice over the telephone network takes longer, or transmission errors occur. In general, you will achieve shorter delays by switching the call type to Fast (see: Switching the Calltype).

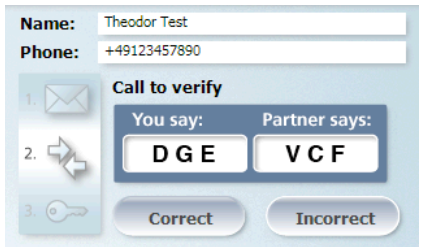
Reasons for longer than normal delay are usually either bad GSM coverage or network congestion. Network congestion can often be circumvented by setting up the call again, sometimes you just get a »bad line«. The GSM data call mode, used by the CryptoPhone to transport the encrypted voice data during a call, has a certain delay, caused by the architecture of the GSM network. The GSM network handles data with lower priority and less error correction than voice transmissions.

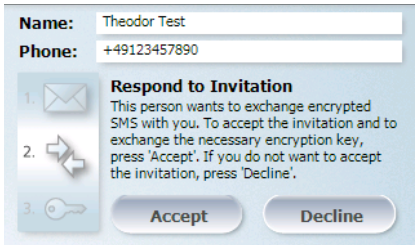
So even if the delay indicator is green, there is always a certain noticeable delay, much like on some transcontinental phone calls. If the overall line quality becomes bad, the delay rises and you may experience »drop outs«. Note that the quality on international calls might not be as good as on domestic calls. The multiple operators involved in an international call often try to minimize their costs by technical measures that can affect



When you press the "Call" button, a phone call to your partner will be initiated. **Make sure to write down the six letters before pressing "Call".** Talk with your partner and read to him the three letters in the "You say" field. Then verify that the three letters in the "Partner says" field match the letters your partner reads to you. This procedure makes sure, that you and your partner are indeed operating on the same key and no man-in-the-middle attack has occurred.

The key is then stored encrypted in the secure storage and used to encrypt and decrypt SMS exchange with your partner. The key from the key exchange is not used directly, but as a "parent key" from which a session key is derived by way of a cryptographic hash function (SHA256). This provides an added layer of cryptographic security.



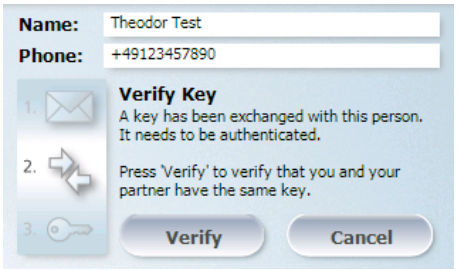

Name:
Theodor Test
Phone:
+49123457890
Respond to Invitation
This person wants to exchange encrypted SMS with you. To accept the invitation and to exchange the necessary encryption key, press 'Accept'. If you do not want to accept the invitation, press 'Decline'.
Accept
Decline

Your CryptoPhone will then generate a public-private key pair using the Diffie-Hellman algorithm and send an invitation SMS to your partner. On the partners phone, a message is shown, that informs your partner that you want to start a key exchange.. Your partner can then either accept or decline the invitation.

If your partner accepts the invitation, his phone will calculate its part of the key exchange and send your partners public key back to you by SMS. In return, your phone will automatically send the Diffie-Hellman response to your partner.

After the key exchange calculation has been completed a window pops up, asking you to verify the key.

You can either verify the key with a phone call or by other means (like when you are meeting with your partner anyway). Choose either “Call to Verify” or “Other”.



the quality of the call. If the call quality is unacceptable, please try calling again. Call quality can also be adversely affected when using certain GSM providers. It often helps to switch the GSM provider to achieve better secure call quality. As a rule of thumb, the larger operators tend to work better then the small ones.

If the Delay indicator becomes reddish or red, please try to find a place with better GSM coverage. Use the signal strength indicator on the right upper side of the display to find a better spot. If the delay indicator turns and stays solid red, please hang up and set up the call again. When no call is in progress, the delay indicator is shown grey.

Secure Calls while moving

When using the GSMK CryptoPhone while moving fast in a car or a train, you may experience a degradation in call quality, periods of longer delay (especially in Robust call mode) and short dropouts during a call. These effects are the result of a so called handover that occurs when you move from the coverage zone of one GSM tower (also called 'GSM cell') to the next. During the handover the data connection is briefly interrupted.

The GSMK CryptoPhone 300 has been successfully tested traveling at speeds faster then 180km/h. The frequency and intensity of disturbances is primarily determined by the GSM network. In rural areas, the network consists of fewer and bigger cells, resulting in

less frequent handovers and less disturbances. In urban areas the network has typically a high density of small cells, resulting in many handovers when moving and thereby causing more disturbances.

Note: In many countries the use of mobile phones while driving is regulated or completely prohibited. You are responsible for complying with local laws and regulations on telephone use while driving a car. The use of the enclosed headset while driving is strongly recommended, even if local regulations may not require this.

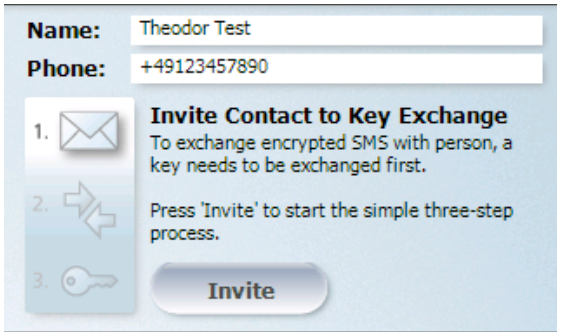
Switching the Calltype

The CryptoPhone 300 supports two different types of call.
They are called them Fast (or Transparent) and Robust (or Non-Transparent).
Technically speaking, the Robust mode uses a special type of error correction in the GSM network, which causes less dropouts (short interruptions) in the conversation, but can cause longer delay under bad conditions and buildup of delay in the network. The Fast mode does not use this error correction and thus has less delay and no delay buildup. However, under certain network conditions it can cause chopped up conversations with lots of dropouts or does not work at all (like on some international calls or calls between different mobile phone operators. In most circumstances the Fast mode gives better call quality. Only if it does not work or gives unsatisfactory results, you should switch to Robust mode.

and regulations. For information how to switch the phone to offline mode (also called flight mode), please consult separate phone hardware manual.

CryptoPhone SMS

An important new feature in the CryptoPhone 300 are encrypted Short Messages (also called texts or SMS). The SMS are encrypted with the same algorithms and key length as the CryptoPhone calls. To start communication via SMS with a partner, you initially need to run a key exchange with your partner. The key exchange for CryptoPhone SMS is only required before the first CryptoPhone SMS can be sent or received. After the key exchange, the key material is stored encrypted in the Secure Storage.



Key Exchange for CryptoPhone SMS

To initiate the key exchange, double tap your partners entry from the CryptoPhone Contacts and press the “Invite” button on the screen.

Changing the volume

To change the audio volume during a Secure Call, use the volume control slider on the left side of the phone. An on-screen indicator will provide you with visual feedback regarding the volume you set. The CryptoPhone 300 volume can be changed over a very wide range to accommodate for different sound characteristics of the CryptoPhone the other party uses. When not in a CryptoPhone call, the volume slider changes the CryptoPhone ring volume.

Mute during call

To mute the microphone during a call, press the button with the crossed out microphone in the screen. To switch the microphone back on again, press the button again.

General Mobile Phone Security Advice

The use of mobile phones and other radio transmission equipment in certain areas is prohibited or restricted. Because of the risk of interference with life-support equipment, the use of mobile phones is also banned in most hospitals. Using a mobile phone in an airplane is a felony in most countries. You are responsible for complying with local laws

To switch the call type, in the Main Screen, click the little icon in the upper left corner and choose Settings from the pulldown menu. Now go to the Connections tab and click the CSD Line Type icon. Here you can choose either Transparent or Non-Transparent in the Connection element selection. Press OK in the upper right corner to store the setting.

Switching the Linetype

Normally, the CryptoPhone uses the V.110 circuit switched data (CSD) - also called digital data call - bearer type to establish a secure connection. To call to an analog landline or to a CryptoPhone on a satellite network or a network with improper data-call configuration (like most GSM carriers in the USA), you can switch to the V.32 bearer mode.

To switch the call type, in the Main Screen, click the little icon in the upper left corner and choose Settings from the pulldown menu. Now go to the Connections tab and click the CSD Line Type icon. Here you can choose either 9600bps (v.32) or 9600bps (v.110) in the Data rate selection. Press OK in the upper right corner to store the setting.

A small 'desktop phone' icon in the CryptoPhone screen will show up if V.32 is activated. The call setup with V.32 takes longer then with V.110, as the modems need some time to synchronize. Incoming calls are not affected by the call type settings.

Problems with setting up a Secure Call

Some providers restrict the reception of GSM data calls, such as needed for the CryptoPhone. The practice is becoming increasingly rare, but a GSM-provider may only allow incoming data calls to subscribers that have a special 'data subscription', which comes with a special second phone number to call to reach the CryptoPhone. Some providers may not recognize that a number you are calling is a GSM/ISDN number, and erroneously try to handle the call via a modem. This can be recognized by the called party because he/she hears a modem sound when picking up the phone. Some providers may not pass data calls to some or all other providers.

Under certain circumstances, especially when roaming in GSM networks that are not properly configured, the "never ending key setup" problem may occur. The phenomenon is that the key setup phase takes longer then 30 seconds and never comes to an end. The underlying technical problem resides in the GSM network. Data calls are sometimes set up but then fail to transport any data.

All of the above conditions may make it impossible to use the CryptoPhone in one or both directions between two CryptoPhones. To by-pass this problem if you are roaming, try switching providers. If secure calling only works in one direction, you could use an unencrypted call to tell the other party to call you using CryptoPhone. These problems

are inherent to using the CSD data call facility and apply to all encrypted telephony over GSM.

To work around these network problems it is recommend that you try out which combination of Calltype and Linetype setting will work in the specific situation. In the USA, for instance, the Linetype nearly always needs to be V.32, while in Europe V.110 works best. Switching the GSM operator also often helps.

For customers in Europe, North Africa and Asia who experience persistent connectivity problems, GSMK can offer the CryptoPhone solution for the Thuraya satellite system. It provides the added benefit of affordable secure communication outside GSM covered areas. A CryptoPhone solution for certain Inmarsat satellite terminals is also available for operations outside GSM or Thuraya coverage.

Sometimes a specific condition of the GSM network may lead to an unclear signaling state in the GSM part of the CryptoPhone, which also might cause the "never ending key setup"-problem or other undesired behavior. This condition can most of the time be fixed by just switching the CryptoPhone off and on again. If you experience this problem more often, activate the “Reset Radio after Call” function, in the CryptoPhone Settings.